Million-Dollar Mathematics

An Honors Thesis (HONRS 499)

by

Holly D. Trietsch

Thesis Advisor
Dr. John Lorch

John Lorch 04/25/03

Ball State University
Muncie, Indiana

March 2003

Graduation: May 3, 2003

HONORS THESIS ABSTRACT

This examination explores three of the challenging "Millennium Prize Problems" that were announced in 2000 by the Clay Mathematical Institute of Cambridge, Massachusetts. They are offering a $1 million prize for the solution to any one of the seven long-standing mathematical questions as a way to "celebrate mathematics in the new millennium" (www.claymath.org). The first section investigates the zeros of the Zeta Function to consider the Riemann Hypothesis. In the second section, the P versus NP problem is examined to try to determine if these two classes of mathematical problems are actually the same. The third section deals with the Birch and Swinnerton-Dyer Conjecture, explaining This investigation of these very difficult problems is meant to explain the statements of each problem, provide any background information, and explore related examples to establish a foundation about some of most significant and interesting mathematical problems of the new millennium.

A special thanks is owed to Dr. John Lorch, my thesis advisor, for devoting so much time and effort to guide me through this process. Thank you Dr. Lorch for challenging me to investigate this topic and offering your expertise in mathematics. I could not have done it without you!

Millennium Prize Problems

To celebrate mathematics of the new millennium, the Clay Mathematics Institute of Cambridge, Massachusetts has named seven "Millennium Prize Problems" that are central to mathematics. These problems are long-standing mathematical questions that still have not been solved after many years of serious attempts by different experts. The institute is offering a one million dollar prize for the solution to any one of these problems.

These "Millennium Prize Problems" were announced in May of 2000, which is 100 years after David Hilbert gave a famous lecture raising some difficult mathematical problems at the Second International Congress of Mathematicians. David Hilbert was a great mathematician that gave numerous contributions to mathematics including theory of invariants, geometry, theory of algebraic number fields, and wrote many important books. Hilbert is now remembered as "one of the greatest mathematicians of the twentieth century." (http://www.claymath.org/prizeproblems/history.htm)

In Hilbert's lecture in 1900, he formulated and presented 15 difficult problems that guided much of the research of mathematicians in the last century. Today, 12 of the 15 problems have been solved, and only one problem, the Riemann Hypothesis, is still as challenging. This problem of trying to prove the Riemann Hypothesis is "now widely regarded as the most important open problem in pure mathematics." (http://www.claymath.org/prizeproblems/history.htm)

THE RIEMANN HYPOTHESIS

THE RIEMANN HYPOTHESIS

The Riemann Hypothesis is a proposition about the zeros of the Riemann zeta function, developed by G.F.B. Riemann (1826-1866). This function, denoted by zeta(s) for complex numbers $s = \sigma + it$, is a complex analytic function defined on the entire complex plane except at s=1. In case that $\sigma > 1$, zeta(s) is given by the following series:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \Rightarrow \zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots.$$

for complex number $s = \sigma + it$. (Granville 14)

This zeta function, valid when $\sigma > 1$, is equal to the Euler Product:

$$\zeta(s) = \prod_p \frac{1}{1 - p_k^{-s}}$$ where $\{p_1, p_2, p_3, \ldots\}$ are primes (Bombieri 2)

The first problem I studied was showing that the zeta function did in fact equal the Euler Product for s > 1.

Problem 1: For s > 1, show $\zeta(s) = \prod_p \frac{1}{1 - p_k^{-s}}$ where $\{p_1, p_2, p_3, \ldots.\}$ are primes. (Bellman 58)

First, $\frac{1}{1 - p_k^{-s}} = \sum_{m=0}^{\infty} p_k^{-ms}$ since $\sum_{m=0}^{\infty} p_k^{-ms}$ is a geometric series

and $\frac{1}{1 - p_k^{-s}}$ is its sum.

Continue with problem 1: For s > 1, show $\zeta(s) = \prod_p \frac{1}{1 - p_k^{-s}}$

Rewrite the zeta function by definition on the left, and expand the product on the right.

$$\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots = \left(\frac{1}{1 - \frac{1}{2^s}}\right)\left(\frac{1}{1 - \frac{1}{3^s}}\right)\left(\frac{1}{1 - \frac{1}{5^s}}\right)\ldots$$

Use the information proved above to rewrite each factor on the right side of the equation.

$$\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots = \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \frac{1}{2^{3s}} + \ldots\right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \frac{1}{3^{3s}} + \ldots\right)\left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \frac{1}{5^{3s}} + \ldots\right)\ldots$$

Multiply on the right side.

$$\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots = 1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \frac{1}{2^{3s}} + \ldots + \frac{1}{3^s} + \frac{1}{2^s 3^s} + \frac{1}{2^{2s} 3^s} + \ldots + \frac{1}{3^{2s}} + \frac{1}{2^s 3^{2s}} + \ldots$$

Write these as summations.

$$\sum_{k=1}^{\infty} \frac{1}{k^s} = 1 + \sum_{n=1}^{\infty} \frac{1}{(p_{j_1}^{t_1} \ldots p_{j_n}^{t_n})^z} \quad \text{where } j_1 < j_2 < \ldots < j_n \text{ and } (t_1, \ldots, t_n) \in Z_+^n$$

By the Fundamental Theorem of Arithmetic, these are equal. In other words, writing the denominators on the left side of the equation in prime factorization will equal the right side of the equation after multiplying the infinite sums. Hence, the zeta function is equal to Euler's Product for s>1.

To become more familiar with the zeta function, I also worked through other problems dealing with this function.

Problem 2:

Prove that $\zeta^2(s) = \sum_{n=1}^{\infty} \frac{d(n)}{n^s}$ for s $\in \Re$, where d(n) is the number of divisors of n. (Conway 194)

$$\zeta^2(s) = \zeta(s)\zeta(s)$$

Rewrite the zeta functions as summations.

$$= \sum_{k=1}^{\infty} \frac{1}{k^s} \cdot \sum_{l=1}^{\infty} \frac{1}{l^s}$$

Combine the summations.

$$= \sum_{k=1}^{\infty} \sum_{l=1}^{\infty} \frac{1}{(kl)^s}$$

Let $kl = n$, (n is the product of k and l)

$$= \sum_{n=1}^{\infty} \sum_{k|n} \frac{1}{n^s}$$

$$= \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{k|n} 1$$

$$= \sum_{n=1}^{\infty} d(n) \frac{1}{n^s}$$

Problem 3:

Prove that $\zeta(s)\zeta(s-1)=\sum_{n=1}^{\infty}\frac{\sigma(n)}{n^s}$, where $\sigma(n)$ is the sum of the divisors of n. (Conway 194)

Write the zeta functions as summations.

$$\zeta(s)\zeta(s-1)=\sum_{k=1}^{\infty}\frac{1}{k^s}\sum_{l=1}^{\infty}\frac{1}{l^{s-1}}$$

$$=\sum_{k=1}^{\infty}\frac{1}{k^s}\sum_{l=1}^{\infty}\frac{l}{l^s}$$

$$=\sum_{k=1}^{\infty}\sum_{l=1}^{\infty}\frac{l}{(kl)^s}$$

$$=\sum_{n=1}^{\infty}\sum_{k}\frac{l}{(n)^s} \quad \text{such that } kl = n$$

$$=\sum_{n=1}^{\infty}\sum_{k}\frac{l}{(n)^s} \quad k \text{ such that } k|n$$

$$=\sum_{n=1}^{\infty}\sum_{k}\frac{\frac{n}{k}}{n^s}$$

$$=\sum_{n=1}^{\infty}\sum_{k}\frac{k}{n^s}$$

$$=\sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{k|n}k$$

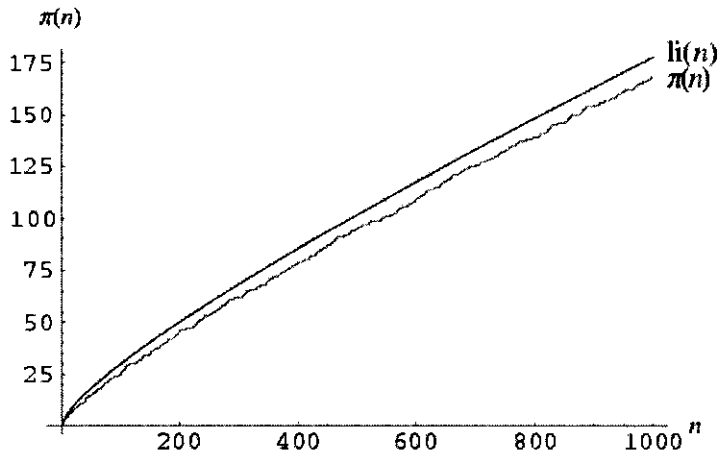
$$=\sum_{n=1}^{\infty}\frac{\sigma(n)}{n^s}$$

When $Re(s) > 1$, the series determining the zeta function converges, where Re(s) means the real part of the complex number s. However, to understand the Riemann Hypothesis, it is important to think about the zeta function having a domain of the whole complex plane except $s = 1$, instead of just when $Re(s) > 1$.

The Riemann zeta function can be extended to the whole complex plane through analytic continuation, except at $s = 1$ where there is a pole. Analytic continuation: Let f_1 and f_2 be analytic functions on domains D_1 and D_2 respectively, and suppose that the intersection of the domains is not empty and that $f_1 = f_2$ on the intersection. Then f_2 is called an analytic continuation of f_1 to D_2 and vice versa. (http://mathworld.wolfram.com/AnalyticContinuation.html) In other words, a function is the analytic continuation of the zeta function if this function is exactly the zeta function for $Re(s)>1$.

The importance of the Riemann Hypothesis and zeta function is due to their relationship to the prime numbers. Remember, prime numbers are numbers that have only two factors, one and itself. (Primes: 2, 3, 5, 11, ...) Prime numbers play an important role in mathematics. The distribution of these prime numbers among all of the natural numbers does not follow a pattern. However, the behavior of this Riemann zeta function is very closely related to the frequency of prime numbers. (http://www.claymath.org/prizeproblems/riemann.htm)

The prime counting function $\pi(n)$ counts the number of primes less than some integer n. For example, $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 2$. As suggested by Gauss in 1791, the prime number theorem gives an approximation of this prime counting function as $\pi(n) \approx \frac{n}{\ln n}$. He refined it to $\pi(n) \approx li(n)$, where *li(n)* is called the logarithmic integral, given by $\int_1^n \left(\frac{1}{\log(t)}\right) dt$. Upon integration by parts, $\frac{n}{\ln n}$ may be considered the leading term of *li(n)*, which provides a somewhat better estimate of $\pi(n)$ than $\frac{n}{\ln n}$ by itself. The following graph illustrates how close these functions are for counting prime numbers.



http://mathworld.wolfram.com/PrimeNumberTheorem.html

It has been found that for small n, $\pi(n) < li(n)$. However, Skewes proved that $\pi(n) > li(n)$ before $n = 10^{10^{10^{34}}}$. (http://mathworld.wolfram.com/PrimeNumberTheorem.html)

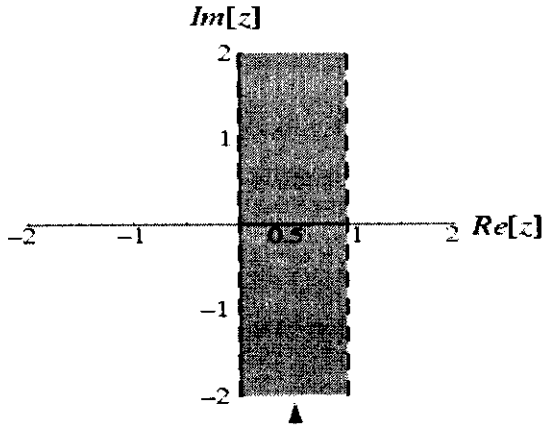
In any case, the specific content of the Prime Number Theorem is that the limit of the prime counting function divided by either of these estimates will equal one.

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

If the Riemann Hypothesis is proven, we will have a better idea about the error in this approximation and gain more knowledge about the distribution of prime numbers.

The zeros of the zeta function are the values of complex number s for which $\zeta(s) = 0$. These zeros occur at negative even integers {-2, -4, -6,...}. These zeros are referred to as the trivial zeros. (Granville 14)

All of the other zeros of the zeta function are called the nontrivial zeros and occur when $0 < \sigma < 1$ for the complex number $s = \sigma + it$. This area on the complex plane when $0 < \text{Re}(s) < 1$ is called the critical strip. (Conway 193)



critical strip

http://mathworld.wolfram.com/CriticalStrip.html

This leads us to the Riemann Hypothesis that all zeros of the zeta function within the critical strip satisfy Re(s) = ½. So, if $\zeta(s) = 0$ and $0 \leq \text{Re}(s) \leq 1$, then Re(s) = ½. This means that all of the nontrivial zeros would lie on the line Re(s) = ½. (Granville 14)

In 1974, Levinson showed that at least 1/3 of the zeros of the zeta function must lie on the line Re(s) = ½. This result has since been sharpened to 40% of all the zeros. (http://mathworld.wolfram.com/RiemannHypothesis.html)

In 1986, it was shown that the first 1.5 billion nontrivial zeros of the zeta function are in fact on this line Re(s) = ½. (http://www.utm.edu/research/primes/notes/rh.html) A proof of this hypothesis for **all** the nontrivial zeros can win the one million dollar prize offered by the Clay Mathematics Institute.

Since the Riemann Hypothesis is that all of the zeros in the critical strip are on the line Re(s) = ½, I looked at the problem of showing that the zeta function has no zeros outside of the critical strip except the trivial zeros. To solve this problem, one begins by showing that the zeta function has no zeros for Re(s) > 1.

Problem 4: Prove $\zeta(s) \neq 0$ for Re(s) > 1.

Let $F(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ and $G(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ (Represented by Dirichlet series)

$f(n) = 1$ $g(n) = \mu(n)$

Since F(s) and G(s) converge absolutely for Re(s), then

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s} \quad \text{where } h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{d|n} 1 \cdot \mu\left(\frac{n}{d}\right)$$

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{\sum_{d|n} \mu\left(\frac{n}{d}\right)}{n^s}$$

However, $\sum_{d|n} \mu\left(\frac{n}{d}\right) = \left[\frac{1}{n}\right]$ where $\mu(n)$ is a Mobius Function

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{\left[\frac{1}{n}\right]}{n^s} = 1 \qquad \text{If } n = 1, \left[\frac{1}{n}\right] = 1 \qquad \text{If } n > 1, \left[\frac{1}{n}\right] = 0$$

$F(s)G(s) = 1$ for Re(s) > 1

$$\zeta(s) \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1 \quad \text{for Re(s)} > 1$$

$\therefore \zeta(s) \neq 0$ for Re(s) > 1

(Apostol 228-229)

In order to use the previous problem (Problem 4) to show that the zeta function has no zeros except the trivial zeros outside of the critical strip, one needs to employ the functional equation for the zeta function.

Functional Equation: $\zeta(s) = 2(2\pi)^{s-1}\Gamma(1-s)\zeta(1-s)\sin\left(\frac{\pi}{2}s\right)$ (Conway 192)

This equation relates the zeta function to the gamma function Γ. This function has several properties, of which the most useful for this is that Γ (s) has no zeros. When analytic continuation is used to extend the domain of the zeta function, $\zeta(s)$ is differentiable on the entire complex plane except at s = 1. Therefore, the problem is basically to show that the only zeros of $\zeta(s)$ outside of the critical strip are s = -2, -4, -6, ... (the trivial zeros).

If Re(s) > 1, $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ Since $\mathrm{Re}(\sum_{n=1}^{\infty} \frac{1}{n^s}) \neq 0$

$$\left[\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots \Rightarrow 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots \neq 0\right]$$

Then $\sum_{n=1}^{\infty} \frac{1}{n^s} \neq 0$ and therefore, there are no zeros of $\zeta(s)$ when Re(s)>1

If Re(s) < 0, there are 2 cases:

1. Let s = -2n, then the functional equation:

$$\zeta(-2n) = 2(2\pi)^{-2n-1}\Gamma(1+2n)\zeta(1+2n)\sin\left(\frac{\pi}{2}\cdot -2n\right)$$

$$\neq 0 \qquad \neq 0 \qquad = 0$$

since Γ has no zeros; since it is sin of multiples of π

$$\Rightarrow \zeta(-2n) = 0$$

Therefore, when s is a negative multiple of 2, the zeta function has a zero (-2, -4, -6, ….).

2. Let s ≠ -2n, then the functional equation:

$$\zeta(s) = 2(2\pi)^{s-1}\Gamma(1-s)\zeta(1-s)\sin\left(\frac{\pi}{2}s\right)$$

$$\neq 0 \qquad \neq 0 \qquad \neq 0$$

$$\Rightarrow \zeta(s) \neq 0$$

Therefore, when s is not an even negative number, the zeta function does not have any zeros. Thus, the zeta function has no nontrivial zeros outside of the critical strip.

Proving the Riemann Hypothesis, that all of the nontrivial zeros of the zeta function occur when Re(s) = ½, is very important to better understand the distribution of primes. "The failure of the Riemann hypothesis would create havoc in the distribution of prime numbers, [which] singles out the Riemann hypothesis as the main open question of prime number theory." (Bombieri 4)

Bibliography

Apostol, Tom. Introduction to Analytic Number Theory. New York: Springer-Verlag New York, Inc, 1976.

Bak, Joseph and Donald J. Newman. Complex Analysis. NewYork: Springer-Verlag New York, Inc, 1982.

Bellman, Richard. Analytic Number Theory: An Introduction. Massachusetts: The Benjamin/Cummings Publishing Company, Inc, 1980.

Bombieri, E. "Problems of the Millennium: The Riemann Hypothesis."

Chowla, S. The Riemann Hypothesis and Hilbert's Tenth Problem. New York: Gordon and Breach Science Publishers, Inc, 1965.

Conway, John B. Functions of One Complex Variable. New York: Springer-Verlag, New York, Inc, 1978

Granville, Andrew. "Prime Possibilities and Quantum Chaos." Mathematical Sciences Research Institute Emissary Magazine p.12-18

P VERSUS NP

THE P VERSUS NP PROBLEM

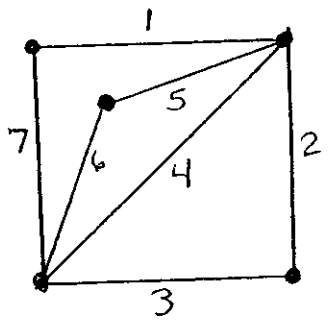
The P vs. NP problem is the biggest open question in theoretical computer science. This problem in computational complexity theory plays a very important role in modern cryptography (Cook 9) To understand this problem, it is important to understand what P and NP mean.

P stands for polynomial time and is a class of languages solvable in polynomial time, where a language is simply a problem with a "yes/no" answer (Ramachandran). Polynomial time is when the execution time of a computation is no more than a polynomial function of the problem size, as measured by the number of inputs required to enter the original problem. You can prove that a problem is in P by showing an algorithm that solves it in polynomial time.

NP stands for nondeterministic polynomial time and is a class of languages that have a polynomial time verification algorithm. An algorithm is a method to compute the correct answer to an input. This just means that a proposed solution to an NP problem can checked in polynomial time, but to solve the problem takes longer than polynomial time. A nondeterministic Turing machine, introduced by Alan Turing in 1936, can verify a solution in polynomial time (Cook 1).

To better understand this, here are a few examples.

Given a graph that has v vertices and m edges, we can ask ourselves if the graph has an Euler Tour. (This is an example of a problem with a "yes/no" answer.) A graph has an Euler Tour if and only if it is possible to walk along the edges of the graph from point to point and return to the starting point by traversing each edge exactly once. This graph with 5 vertices and 7 edges has an Euler Tour (Ramachandran):

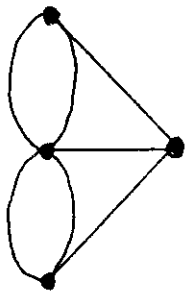


For m edges,
m!-time algorithm.

NP problem

To look for an Euler Tour we can look at all of the possible routes. Therefore, to see if a graph with m edges has an Euler Tour will be an m!-time algorithm. This is not a polynomial time algorithm and hence to see if a graph has an Euler Tour this way is an NP problem.

However, Euler came up with a polynomial time algorithm for this Euler Tour problem. It states that a graph has an Euler Tour if and only if every vertex has an even number of edges on it (Ramachandran). Using this algorithm, it is easily determined if this graph has an Euler Tour.

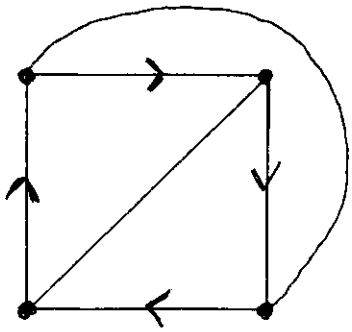


Each vertex has an odd number of edges.

Now, a P problem

Therefore, Euler made the Euler Tour problem a polynomial-time problem, and thus it is now a P problem.

Another problem to consider is if a graph has a Hamiltonian Cycle. A graph has a Hamiltonian Cycle if it is possible to walk along the edges of the graph from vertex to vertex and return to the starting point by traversing each *vertex* exactly once (Ramachandran). Notice that this graph does have a Hamiltonian Cycle:

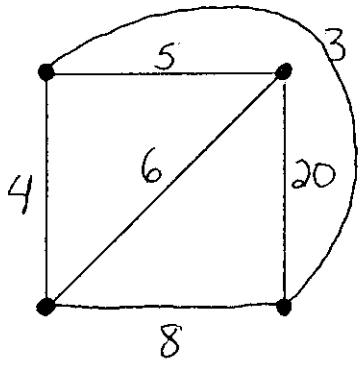


For n vertices, n!-time algorithm.

NP problem

To figure out if a graph of n vertices has a Hamiltonian Cycle has n! steps. The difference between this problem and the Euler Tour problem is that no one knows how to solve the Hamiltonian Cycle problem in a polynomial number of steps. Therefore, this problem is an NP problem since we cannot solve it in polynomial time, but we would be able to check a possible solution in polynomial time.

The last example is closely related to the Hamiltonian Cycle problem, and is called the Traveling Salesman Problem. This is the most famous problem in connection to the P vs. NP problem. This problem asks, given a graph with a cost on each edge, together with a "budget" value B, is there a Hamiltonian cycle in the graph whose total cost is less than the budget B? An example would look like the graph from the Hamiltonian Cycle problem, but with costs on each edge.



Budget = 25

Again, NP problem

Again, this problem does not have a polynomial time algorithm, so it is NOT a P problem.

Since P problems not only can be solved in polynomial time, but can also be checked in polynomial time, all P problems are also in NP. Hence, the class of P problems is a subset of the NP problems (Papadimitriou 46).

When trying to understand this problem of P vs. NP, another important class of problems arises. This class is called NP-Complete. A language L is NP-complete if

1) L is in NP
2) Every language L' in NP can be transformed to L in polynomial time

(Papadimitriou 165)

All NP-complete problems are very closely related, since any one of them can be mapped to any other by a reduction in polynomial time. In fact, all known NP-complete languages are in fact polynomially isomorphic (Papadimitriou 332).

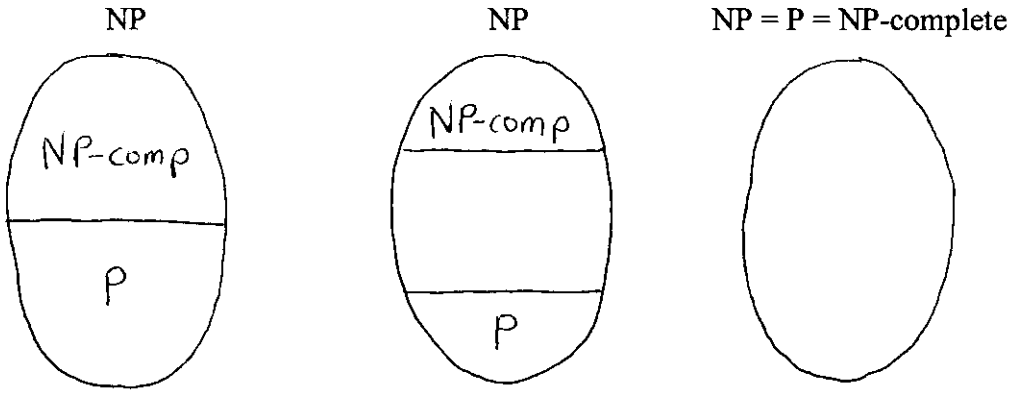
In other words, a problem is said to be NP-complete if the existence of a polynomial time solution for that problem implies that all NP problems have a polynomial time solution. However, "at present, all known algorithms for NP-complete problems require time which is exponential in the problem size" (http://www.widipedia.org/wiki.phtml?title=NP-Complete)

Showing that a problem is NP-complete establishes that it is among the least likely to be in P. (Papadimitriou 182). This is because if the problem did have polynomial time algorithm, we would be able to solve all of the NP problems.

Therefore, if any NP-complete problem turns out to be in P, then P = NP. (http://www.claymath.org/prizeproblems/milliondollarminesweeper.htm) However, at present, all known algorithms for NP-complete problems have exponential time.

On the other hand, if P ≠ NP, then there is a language in NP which is neither in P nor is it NP-complete (Papadimitriou 330).

3 Possibilities



If P ≠ NP

If P = NP

(Papadimitriou 330)

This problem of P versus NP is very important and has significant consequences if it is solved. If it is proven that $P \neq NP$, then a lot of important problems will be proven to be intractable (not solvable in polynomial time). Also, an infinite collection of different classes of problems will lie between P problems and NP-complete problems.

If it is proven that $P = NP$, then numerous problems will have polynomial-time solution algorithms that are now unknown. This would mean that potentially all of the solutions to all of the Millennium Prize problems could be found. However, proving that $P = NP$ would have an even greater consequence of putting the security of public-key cryptography in jeopardy (Cook 9).

Bibliography

Ambos-Spies, Klaus, Steven Homer, and Uwe Schoning. Complexity Theory: Current Research. New York: Cambridge University Press, 1988.

Cook, Stephen. "The P versus NP Problem."

Du, Ding-Zhu and Ker-I Ko. Theory of Computional Complexity. New York: John Wiley & Sons, Inc, 2000.

"NP-Complete." http://www.widipedia.org/wiki.phtml?title=NP-Complete

Papadimitriou, Christos H. Computational Complexity. New York: Addison-Wesley Publishing Company, Inc, 1994.

Ramachandran, Vijaya. Lecture: "The P versus NP Problem." University of Texas in Austin, 2001.

Stewart, Ian. "Million-Dollar Minesweeper." http://www.claymath.org/prizeproblems/milliondollarminesweeper.htm

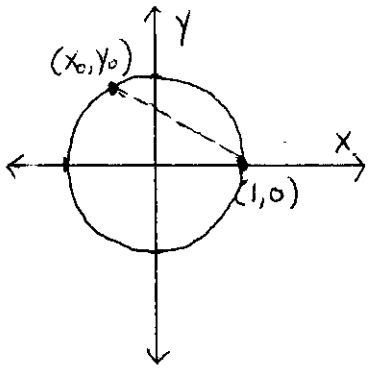
THE BIRCH AND SWINNERTON-DYER CONJECTURE

THE BIRCH AND SWINNERTON-DYER CONJECTURE

The Birch Swinnerton-Dyer Conjecture deals with trying to determine the number of rational points there are on an elliptic curve. (A rational point is a point with rational coordinates.) One of the first problems I did dealt with rational points on a unit circle.

Problem 1:

Show that (x_o,y_o) is a rational point on the unit circle if and only if the slope of the line joining (1, 0) to (x_o,y_o) is rational.



$\Leftarrow$ Let the equation of the line passing through (1, 0) be $x = ty + 1$ where t is a rational number and 1/t is the slope. (Since t is rational, 1/t is also rational.) The other point where this line intersects the unit circle is represented as (x_o,y_o). To find (x_o,y_o) we put $x = ty + 1$ into $x^2 + y^2 = 1$.

$$(ty + 1)^2 + y^2 = 1$$

$$t^2y^2 + 2ty + 1 + y^2 = 1$$

$$t^2y^2 + y^2 + 2ty = 0$$

$$(t^2 + 1)y^2 + 2ty = 0$$

$$(t^2 + 1)y + 2t = 0$$

$$(t^2 + 1)y = -2t$$

$$y = \frac{-2t}{t^2+1}$$

$$x = t\left(\frac{-2t}{t^2+1}\right) + 1$$

$$x = \frac{-2t^2}{t^2+1} + \frac{t^2+1}{t^2+1}$$

$$x = \frac{-t^2+1}{t^2+1}$$

$$\text{Therefore, } (x_o, y_o) = \left(\frac{-t^2+1}{t^2+1}, \frac{-2t}{t^2+1}\right)$$

Since the rational numbers are a field and (x_o, y_o) is in terms of adding or multiplying t (a rational number), (x_o, y_o) has rational coordinates. Hence, (x_o, y_o) is a rational point.

$\Rightarrow$ Let (x_o, y_o) be a rational point. From above, we know that

$$(x_o, y_o) = \left(\frac{-t^2+1}{t^2+1}, \frac{-2t}{t^2+1}\right) \text{ where t is rational.}$$

Then the slope of the line jointing (x_o, y_o) and (1, 0) is:

$$\frac{\frac{-2t}{t^2+1}}{\frac{-t^2+1}{t^2+1}-1} = \frac{\frac{-2t}{t^2+1}}{\frac{-t^2+1}{t^2+1}-\frac{t^2+1}{t^2+1}} = \frac{\frac{-2t}{t^2+1}}{\frac{-2t^2}{t^2+1}} = \frac{-2t}{t^2+1}\cdot\frac{t^2+1}{-2t^2} = \frac{1}{t}$$

Since t is rational, then 1/t is rational. Therefore, the slope is rational.

In order to study the Birch and Swinnerton-Dyer Conjecture, it is important to understand the Hasse Principle. The Hasse Principle basically states that to answer any questions about integer equations, reducing the equation modulo p can be very useful, where p is usually prime. (Rodriguez-Villegas)

An example of this would be to find out if the number $10^{10^{10}} + 3$ is the sum of two square numbers.

Example: Show $10^{10^{10}} + 3$ is the not sum of two square numbers by reducing modulo p.

Start by looking at the square numbers:

1, 4, 9, 16, 25, 36, 49, 64, 81, … which can be reduced modulo 4 to:

1, 0, 1, 0, 1, 0, 1, 0, 1, …(mod 4)

By the division algorithm, any integer can be written in the form $4k + j$ where k, j are integers and $0 \leq j < 4$. Upon squaring, we obtain $4(4k^2 + 2kj) + j^2 = j^2 \pmod 4$. By plugging in the four possible values of j, we see that j^2 is equal to either 0 or 1 (mod 4).

So the sum of squares can be:

$0 + 0 \pmod 4 = 0$

$0 + 1 \pmod 4 = 1$

$1 + 1 \pmod 4 = 2$

Therefore, a sum of two squares can be either 0, 1, or 2 (mod 4), but it can never be 3(mod 4).

Let's reduce the original problem modulo 4:

$10^{10^{10}} + 3 \pmod 4$

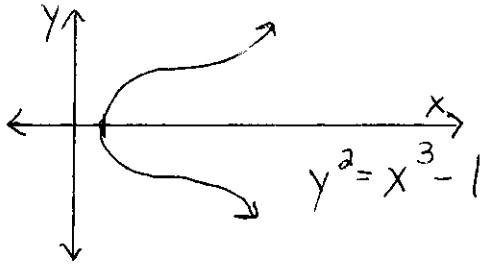
$10^{10^{10}} \pmod 4 + 3 \pmod 4$

$0 + 3 \pmod 4$

$3 \pmod 4$

Therefore, $10^{10^{10}} + 3$ is NOT a sum of two squares since a sum of two squares can never be 3 (mod 4). So this problem was each easier to figure out using reduction modulo p, the idea of the Hasse Principle.

The Birch and Swinnerton-Dyer Conjecture uses the Hasse Principle with elliptic curves. An elliptic curve is given by an equation $y^2 = x^3 + ax + b$ with a, b being integers such that the right hand side of the equation has distinct roots.



An elliptic curve has a degree of 3, and if you draw a line through the curve it will meet the cubic at three points. Given two points that the line goes through, we can find the third point. Also, if the two points are have rational coordinates, the third point will have rational coordinates.

Using the idea of the Hasse Principle, we can count the number of solutions, Np, to an elliptic curve modulo p, where p is a prime number. So, Np is the number of pairs (x, y) (mod p) that satisfy the equation $y^2 = x^3 + ax + b$.

The Birch and Swinnerton-Dyer Conjecture resulted from studying the behavior of $P(x) = \prod_{p \le x} \frac{Np}{p}$. From their numerical evidence, they conjectured that an elliptic curve has infinitely many rational points if and only if this P(x) goes to infinity as x increases. (Rodriguez-Villegas)

Another way to state this conjecture is in terms of a dirichlet series called the L-function. The L-function is given as $L(E,s) = \prod_{primes} Fp(s)^{-1}$ for a given elliptic curve E. It is known that the Euler factors satisfy $Fp(1) = \frac{Np}{p}$. The conjecture in this way states that the elliptic curve E has infinitely many rational points if and only if this L-function goes to zero when s=1. (Rodriguez-Villegas)

The Birch and Swinnerton-Dyer Conjecture is important because it helps us know some information about curves of genus 1. To picture what genus 1 means, think of a donut since it has one "hole" in the middle. So a curve with genus 2 would be something like two donuts hooked on the side, hence two "holes."

If we have a polynomial equation with integer coefficients and degree ≤ 2, then it is a curve of genus 0 and has either no or infinitely many rational points. (The genus of a curve describes the shape of the complex solutions.)

Also, the Mordell Conjecture, proven in 1983 by Faltings, gives us information about curves of genus ≥ 2. It states that if the genus of a polynomial equation is ≥ 2, then the set of rational points on the curve is finite (Wiles 1).

The Birch and Swinnerton-Dyer Conjecture, if proven, would "fill the gap" between what is known about rational curves of genus 0 and curves of genus ≥ 2. Again, the conjecture tells us that an elliptic curve of genus 1 has infinitely many rational points if and only if $\prod_{p \leq x} \frac{Np}{p}$ goes to infinity.

As Birch and Swinnerton-Dyer examined $\prod \frac{p}{N_p}$ for elliptic curves, I computed and interpreted $\prod \frac{p}{N_p}$ for a less complex case, namely for the curve $x^2 + y^2 = 1$. . In order to do this, we must first look at a few Lemmas, articulated by Dr. John Lorch, my thesis advisor.

Lemma 1: *All solutions to $x^2 + y^2 = 1$ in Z_p other than (1, 0) are parametrized by*

$((t^2 - 1)(1 + t^2)^{-1}, 2t(1 + t^2)^{-1})$, *where $t \in Z_p$ with $t^2 \neq -1$.*

(p denotes a positive prime number)

Proof: Since (1, t) is not a solution to $x^2 + y^2 = 1$ for any $t \neq 0$ in Z_p, we may deduce that any other solution to the equation must lie on some line $y = t(x - 1)$ where $t \in Z_p$. Let (x_o, y_o) be such a solution. Using substitution, we obtain

$$(1 + t^2)x_o^2 - 2t^2x_o + (t^2 - 1) = 0 \text{ in } Z_p. \qquad (1)$$

If $t^2 = -1$, one obtains $x_o = 1$ and $y_o = 0$, which is the solution we already have. However, if $t^2 \neq -1$, then by multiplying equation (1) by $(1 + t^2)^{-1}$ and factoring, one obtains $x_o = 1$ or $x_o = (t^2 - 1)(t^2 + 1)^{-1}$. Now putting the second value of x_o into the equation $y = t(x - 1)$ to obtain $y_o = 2t(t^2 + 1)^{-1}$.

Lemma 2: *If -1 is a square in* Z_p, *then* $x^2 + y^2 = 1$ *has p-1 solutions in* Z_p. *Otherwise, there are p+1 solutions.*

Proof. First, let's suppose -1 is not a square in Z_p. Then, by Lemma 1, the solutions to $x^2 + y^2$ consist of (1, 0) together with pairs of the form $((t^2 - 1)(1 + t^2)^{-1}, 2t(1 + t^2)^{-1})$, where we allow t to assume *any* of the p values in Z_p. We will finish if all of these pairs are distinct, which is the case seen by examining the pairs $(t^2 - 1, 2t)$. Thus, we have a total of $p + 1$ solutions.

Now we should address the case where -1 is a square in Z_p. In this case there are two square roots, t_o and $-t_o$, for some $t_o \in Z_p$. Note these roots are distinct and there cannot Be any other roots (since a degree two polynomial in a polynomial ring over a field can have at most two roots in the field.) From Lemma 1, we see that both t_o and $-t_o$ lead to the solution we already have, namely (1, 0). Thus, in addition to (1, 0), we obtain $p - 2$ other solutions by looking at the pairs $((t^2 - 1)(1 + t^2)^{-1}, 2t(1 + t^2)^{-1})$, for $t \in Z_p$ with $t \neq \pm t_o$. These are distinct pairs, for the same reason we have given above. Thus, we have a grand total of $p - 1$ solutions.

Lemma 3: *Suppose now that p is an odd prime. Then -1 is a square in* Z_p *if and only if* $p \equiv 1 \pmod 4$.

Proof. First, suppose $p \equiv 1$ modulo 4, and let g be a generator of the cyclic group Z_p *. Then the order of g is $p - 1$, and it follows that the order of $g^{(p-1)/4}$ is 4. Therefore, $g^{(p-1)/2}$ is a square root of 1 which is not equal to one, and hence $(g^{(p-1)/4}) = g^{(p-1)/2} = -1$. So -1 is indeed a square in Z_p .

Lemma 4: $\sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} = \frac{\pi}{4}$

Proof. Via geometric series, when $|x| < 1$ we have

$$\frac{1}{1+x^2} = \frac{1}{1-(-x^2)} = 1 - x^2 + x^4 - x^6 + \ldots$$

Integration gives $\tan^{-1}(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots$, which converges on the interval (-1, 1]. Evaluating the last equation when x =1 gives, $\tan^{-1}(1) = \frac{\pi}{4}$.

Proposition 1: *For the curve* $x^2 + y^2 = 1$, $\prod \frac{p}{N_p} = \frac{\pi}{4}$.

Proof. First, observe that $N_2 = 2$, and thus $\prod \frac{p}{N_p}$ may be taken over the odd primes. The odd primes may be broken into two categories: those for which -1 is a square in Z_p (in which case $N_p = p - 1$) and those for which it is not (in which case $N_p = p + 1$).

By Lemma 3, these categories correspond to the primes being congruent to 1 or -1 modulo 4, respectively. Therefore, $\prod \frac{p}{N_p} = \prod_{p\equiv 1} \frac{p}{p-1} \prod_{p\equiv -1} \frac{p}{p+1} = \prod_{p\equiv 1} \frac{1}{1-\frac{1}{p}} \prod_{p\equiv -1} \frac{1}{1+\frac{1}{p}}$.

By expanding into geometric series and multiplying, we obtain a sum of terms of the form: $\frac{1}{p_1^{k_1} \ldots p_r^{k_r} \times (-1)^{l_1} q_1^{l_1} \ldots (-1)^{l_s} q_s^{l_s}}$ where the p's are congruent to 1 modulo 4 and the q's are congruent to -1. By the Fundamental Theorem of Arithmetic, every odd number is obtained exactly once in the denominator of the fraction above.

The only question remaining is the sign of the denominator. If the denominator is congruent to 1 modulo 4, then $l_1 + \ldots + l_s$ must be even, and hence the sign is positive. On the other hand, if the denominator is congruent to -1 modulo 4, then $l_1 + \ldots + l_s$ must be odd, and hence the sign is negative. Therefore, using this together with Lemma 4, we find that $\prod_{p\equiv 1} \frac{1}{1-\frac{1}{p}} \prod_{p\equiv -1} \frac{1}{1+\frac{1}{p}} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots = \frac{\pi}{4}$

$\frac{\pi}{4}$ is related to the length of the curve $x^2 + y^2 = 1$ in a way that is similar to the situation on elliptic curves (which have infinite length.)

Bibliography

Knapp, Anthony W. Elliptic Curves. New Jersey: Princeton University Press, 1992.

Koblitz, Neal. Introduction to Elliptic Curves and Modular Forms. New York: Springer-Verlag New York, Inc, 1984.

Rodriguez-Villegas, Fernando. Lecture: "The Birch and Swinnerton-Dyer Conjecture." University of Texas in Austin, 2001.

Wiles, A. "The Birch and Swinnerton-Dyer Conjecture."

PRESENTATION

Department of Mathematical Sciences
Ball State University

Undergraduate Colloquium Series

The Millenium Prize Problems

by

Holly Trietsch

Ball State Student

Abstract: The Clay Mathematical Institute is offering a 1 million dollar prize for the solution to any one of seven difficult and important mathematical problems. We explore several of these problems.

12:30 p.m.
Thursday, December 5, 2002
RB 449

Students may enjoy the pizza served at 12:00 noon.

BALL STATE
UNIVERSITY.

Department of Mathematical Sciences
Ball State University
Undergraduate Colloquium Series

A Series Designed For Students, Organized by
Linda Barton and Ahmed Mohammed

Thursdays 12:30 - 1:00 PM
RB 449

This series will include informal presentations from all areas of the mathematical sciences, geared to a level accessible to undergraduates. Speakers will include faculty, senior students, and guests. A brief question and discussion period will follow each week's presentation.

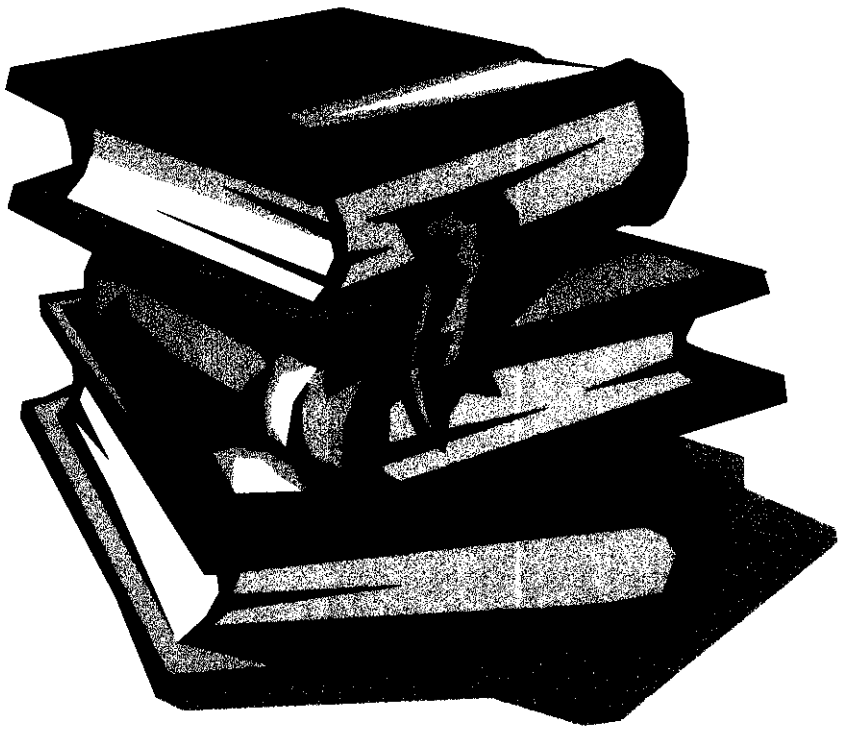
Fall 2002 Schedule

Aug 29	Ryan Lowe	"Breaking the Code"
Sep 12	Diane Vian	"Internship Through Department of Energy"
Sep 26	Ralph Bremigan	" Building the cheapest well between three cities: another notion of the center of a triangle"
Oct 10	Michael Karls	"My Experience at the Johns Hopkins University Applied Physics Laboratory"
Oct 24	Gary Dean	"Inverting Excess Loss Tables"
Nov 07	Sheryl Stump	"What is Mathematics Education?"
Nov 21	Rich Stankewitz	"Fractal Image Compression"
Dec 05	Holly Trietsch	"The Millenium Prize Problems"

Undergraduates who elect to attend the full series and keep a journal may earn one hour credit in Maths 298.

MATH AND PIZZA!

December 5, 2002, in RB 449
12:00 to 1:00 p.m.



- Free pizza will be served from 12:00 to 12:25 p.m. in RB 486.

Presentation:

"The Millenium Prize Problems" at 12:30 p.m. by Holly Trietsch, Ball State student in RB 449.

Millennium Prize Problems

Holly Trietsch

RIEMANN HYPOTHESIS

– Riemann Zeta Function

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\ldots. \quad \text{for} \quad s=\sigma+it$$

$$\zeta(s)=\prod_{p}\frac{1}{1-p_k{}^{-s}} \quad \underline{\text{Euler Product}}$$

– Only Valid if $\sigma > 1$

– $\zeta(s)$ can be extended to whole complex plane through analytic continuation, except at s=1 (pole)

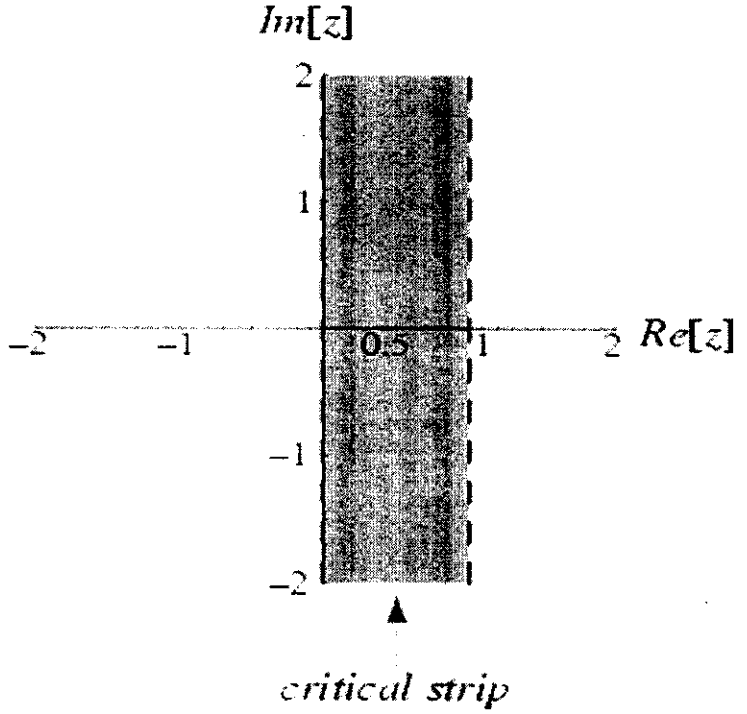
- $\zeta(s)$ is closely related to the frequency of prime numbers

- Prime Number Theorem

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

- If Riemann Hypothesis is solved, we will have better idea about the error in this approximation

- Trivial Zeros of $\zeta(s)$ occur at {-2, -4, -6, …}
- All other zeros, called nontrivial zeros, occur when 0 < Re(s) < 1



- Riemann Hypothesis – All zeros of $\zeta(s)$ within the critical strip lie on the line Re(s) = ½

- Once we have established $\zeta(s) \neq 0$ for Re(s) >1, we can use the functional equation to prove there are zeros only at -2, -4, -6,… when Re(s) < 0

- Functional Equation

$$\zeta(s) = 2(2\pi)^{s-1}\Gamma(1-s)\zeta(1-s)\sin\left(\frac{\pi}{2}s\right)$$

- This Gamma function has NO zeros

Birch & Swinnerton-Dyer Conjecture

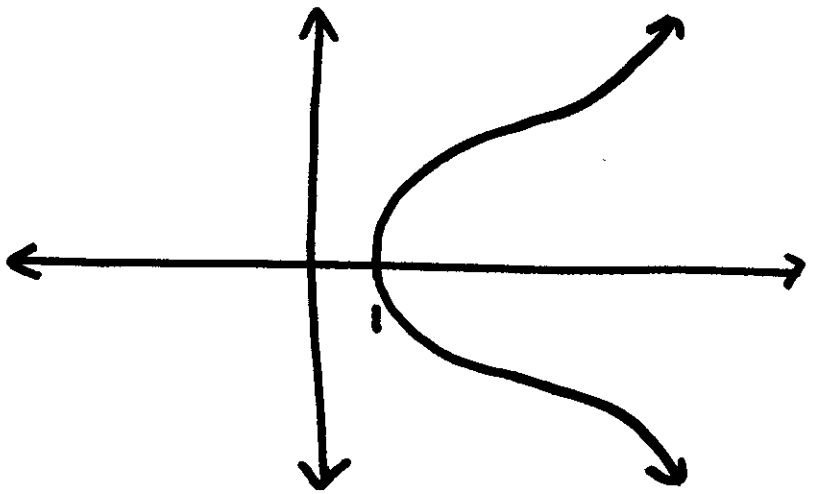
- Deals with trying to determine the number of rational points there are on an elliptic curve

- Hasse Principle – To answer questions about integer solutions to polynomial equations, reducing modulo p can be helpful

- Example - $10^{10^{10}} + 3$ is not the sum of two squares

- Reason – Reduce modulo 4,
  3 is not the sum of two squares in $\mathbb{Z}_4$

- Elliptic Curve $y^2 = x^3 + ax + b$ with integers a and b such that the right hand side of the equation has distinct roots.
- Any elliptic curve carries a group structure



$y^2 = x^3 - 1$

- Np is the number of pairs (x, y) modulo p that satisfies the equation

- BSD Conjecture – From study of $P(x)=\prod_{p\le x}\frac{Np}{p}$ they conjectured that an elliptic curve has infinitely rational points iff P(x) goes to infinity as x increases

- We have calculated this for $x^2+y^2=1$

- It is known that a curve of genus 0 has either no or infinitely many rational points.

- Mordell's Conjecture – If the genus of a polynomial equation is ≥ 2, then the set of rational points on the curve is finite.

- Birch & Swinnerton-Dyer Conjecture, if proven, tells us that a curve of genus 1 has infinitely many rational points if and only if

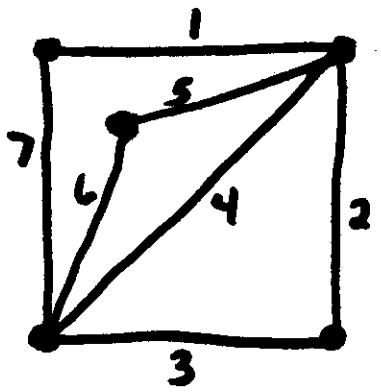
$$\prod_{p \leq x} \frac{Np}{p}$$ goes to infinity

P versus NP

- P (polynomial time) – class of languages solvable in polynomial time
- NP (nondeterministic polynomial time) – class of languages that have a polynomial time verification algorithm
- P is a subset of NP

Euler Tour

- A graph has an Euler Tour if and only if it is possible to walk along the edges of the graph from point to point and return to the starting point by traversing each edge exactly once.

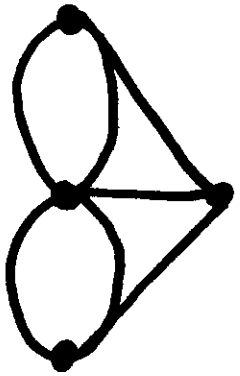


For m edges,

m!-time algorithm

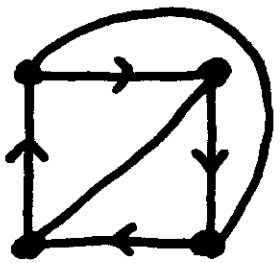
NOT poly-time

- Euler found poly-time algorithm. A graph has an Euler Tour if and only if every vertex has an even number of edges on it.



Hamiltonian Cycle

A graph has a HC if it is possible to walk along the edges of the graph from vertex to vertex and return to the starting point by traversing each *vertex* exactly once.

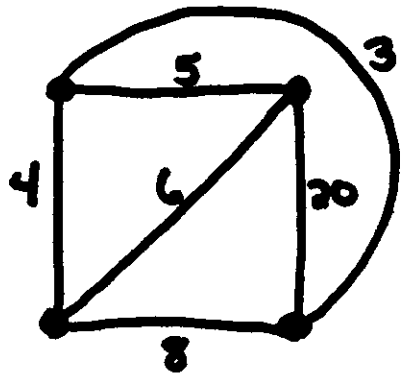


For n vertices,

n!-time algorithm

Traveling Salesman Problem

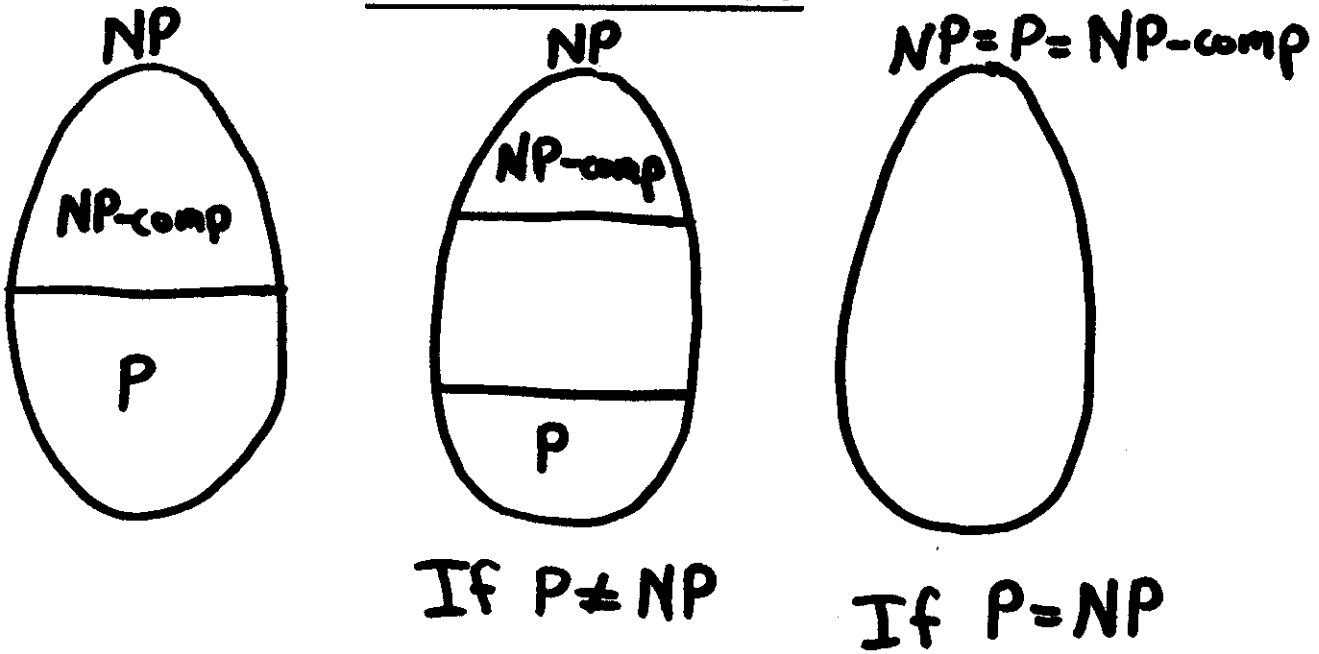
Given a graph with a cost on each edge, together with a budget value B, is there a HC in the graph whose total cost is less than the budget?



B=25

- A languag e L is NP-complete if
  - 1) L is in NP
  - 2) Every language L' in NP can be transformed to L in polynomial time
- If you find a poly-time solution to one NP-complete problem, then you can solve all NP problems in poly-time

3 Possibilities



- If $P \neq NP$:
  - Many important problems will be proven to be unsolvable in polynomial time
  - An infinite collection of different classes of problems will lie between P and NP

- If $P = NP$:
  - Numerous problems will have much faster solution algorithms
  - Security of public-key cryptography will be in jeopardy